UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/701,157	11/22/2000	George Friedman	1206-00	7408

35811 7590 04/07/2006

IP GROUP OF DLA PIPER RUDNICK GRAY CARY US LLP
1650 MARKET ST
SUITE 4900
PHILADELPHIA, PA 19103

EXAMINER	
CALLAHAN, PAUL E	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 04/07/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/701,157	FRIEDMAN ET AL.	
	Examiner	Art Unit	
	Paul Callahan	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 November 2000*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-149* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-6,8,40-47,55-68,95-97,129,130 and 148* is/are rejected.

7)☐ Claim(s) *7,9-39,48-54,69-94,98-128,131-147 and 149* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *22 November 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date ~~_____~~ PC 12-7-05
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This Office Action is a re-mailing of the previous one having a mail date of 12-14-05. In the processing of the previous Office Action for mailing it was mistakenly switched with another Office Action having a different Application / Serial Number: 10/360,794. The time period for response to this Office Action is hereby restarted with the mail date of this Office Action

E-Moise
EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER

2. Claims 1-149 are pending in this application and have been examined.

Claim Rejections - 35 USC § 112

3. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

4. Claim 129 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. The claim is directed towards; "A computer readable medium for monitoring data security..." Without a computer program product stored on the medium, the medium itself is only a blank storage location. The applicant may wish to rewrite the claim in the form of: "A computer program product embodied in a memory medium that when read out directs a system to..."

Claims 130-147 are dependent on claim 129 and each contains a similar preamble directed towards: "a computer readable medium..." or: "a machine readable medium..." or: "a computer readable material..." The claims are therefore rejected based upon their dependency from claim 129, and they are independently rejected on the same 112 2nd indefiniteness basis as is that claim.

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

6. The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

7. Claims 1-5, and 8 are rejected under 35 U.S.C. 102(e) as being anticipated by Saito et al. US 5,848,158.

As for claim 1, Saito teaches a method for maintaining data security comprising: creating a package comprising data and one or more permissions for regulating use of the data; and providing a receiver for processing the package and storing the data in a vault. (col. 2 lines 60-67).

As for claim 2, Saito teaches a method according to claim 1, wherein the step of processing the package further comprises opening the package and verifying the receiver for processing of the package (col. 5 lines 24-45).

As for claim 3, Saito teaches a method according to claim 2 further comprising searching for at least one driver for reading the package (col. 2 lines 45-55 "Program to manage copyright", col. 4 lines 50-60).

As for claim 4, Saito teaches a method according to claim 1 further comprising detecting violations of said one or more permissions (col. 2 lines 56-59).

As for claim 5, Saito teaches a method according to claim 4 wherein the step of providing a receiver further comprises providing internal security (col. 4 lines 50-59).

As for claim 8, Saito teaches a method according to claim 5, wherein step of creating a package further comprises an executable for verifying the operation of the receiver when the package is opened (col. 5 lines 24-45).

8. Claims 95-97, 129, 130, and 148 are rejected under 35 U.S.C. 102(e) as being anticipated by Schneck, US 5,933,498

As for claims 95 and 129, Schneck teaches a system and a computer program product embodied in a memory medium for directing for maintaining data security comprising: a receiver for processing a package comprising data and one or more permissions for regulating use of the data; and a vault for storing the data (fig. 1, col. 15 line 50 through col. 16 line 20).

As for claim 96, Schneck teaches a system according to claim 95 further comprising internal security for protecting the data stored in the vault (col. 15 line 50 through col. 16 line 20).

As for claims 97 and 130, Schneck teaches a system and a computer program product for directing the system according to claim 96, wherein the internal security further detects violation of said one or more permissions (col. 18 lines 10-60, col. 15 lines 20-25).

As for claim 148, Schneck teaches a system for maintaining security during transmission of data between at least two computers comprising: a first computer having a system for creating a package comprising data and one or more permissions selected from a list of available permissions for regulating use of the data; and a second

computer having a system for receiving the package from the first computer, opening the package upon verification and storing the data in a vault (fig.s 1-3, col. 15 line 50 through col. 16 line 20, col. 18 lines 10-60).

Claim Rejections - 35 USC § 103

9. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

10. Claims 6, 40-47, and 55-65 are rejected under 35 U.S.C. 103(a) as being unpatentable over Saito and Saunders US 5,283,828.

As for claim 6, Saito teaches the features of claim 5 on which claim 6 depends, but fails to teach a method according to claim 5, wherein the internal security comprises creating a tag file corresponding to the data and mapping the tag file against the data in a virtual table, with the virtual table including an actual file name of the data and a corresponding tag name for the tag file, wherein the virtual table and the data are stored in the vault. Saunders does teach these features (col. 6 lines 49-59). Therefore it would have been obvious to incorporate these features of Saunders into the system of Saito. It would have been desirable to do so as storage of the virtual table and data in a vault would facilitate more rapid recovery upon decryption, and greater security in the system.

As for claims 40-44 the combination of Saunders and Saito fails to teach a method according to claim 5 for providing data security in a first device driver operably installed in a computer operating system having a layered plurality of device drivers for accessing data in a data storage device, the method comprising, the steps of: detecting an I/O request to said first device driver; determining whether said first device driver is functionally uppermost in the layered plurality of device drivers; if said first device driver is functionally uppermost in the layered plurality of device drivers, performing the I/O request in said first device driver; and if said first device driver is not functionally uppermost in the layered plurality of device drivers, denying the I/O request in said first device driver, and allowing the I/O request to be performed by a next lower level device driver in the layered plurality of device drivers. However Official Notice may be taken that such steps of processing I/O requests to device drivers where the driver is a file system monitor, or where the I/O request comprises decryption or a virus scan, are old and well known in the art. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate these features into the system of Saito and Saunders. It would have been desirable to do so as this would facilitate rapid and secure data processing.

As for claim 45, the combination of Saito and Saunders fails to teach the method of claim 40 wherein the step of determining whether said first device driver is functionally uppermost in the layered plurality of device drivers further comprises the

steps of: determining whether said first device driver has been previously called; if said first device driver has not been previously called, detecting an initial calling module address, storing said initial calling module address, anal concluding that said first device driver is functionally uppermost in the layered plurality of device driver's; if said first device driver has been previously called, detecting a second calling module address, comparing said second calling module address to the initial calling module address, and concluding that said first device driver is functionally uppermost in the layered plurality of device drivers only if the initial calling module address matches the second calling module address. However Official Notice may be taken that such steps are standard in device driver I/O request queuing. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate this feature into the system of Saito and Saunders. It would have been desirable to do so as this would allow for rapid and secure data processing.

As for claims 46 and 47, the combination of Saito and Saunders fails to teach the method of claim 40 wherein the step of denying the 1/O request in the secure first device driver comprises the steps of: setting a first device driver shutdown flag; and initiating a re-hook process, or after the step of detecting an 1/0 request to said first device driver, the steps of: checking whether a first device driver shutdown flag is set; and if said first device driver shutdown flag is set, omitting further steps in said first device driver, and allowing the 1/O request to be performed by a next lower-level device driver in the layered plurality of device drivers. However Official Notice may be taken

that such steps are standard in device driver I/O request queuing. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate this feature into the system of Saito and Saunders. It would have been desirable to do so as this would allow for rapid and secure data processing.

As for claims 55-57, the combination of Saito and Saunders fails to teach a method according to claim 1 further comprising: a port request detection step of detecting a port request for use of a port sent by a process; a process identification step of determining the identity of said requesting process; a process check step of determining if said process should be permitted to access said port; and a permit/deny step of allowing said port request to be fulfilled if said process should be permitted to access said port and denying said port request if said process should not be permitted to access said port, or the method of claim 55 wherein said process check step comprises: a secure process list check step of determining whether said process appears on a list of secure processes, or the method of claim 55 further comprising: a tracking step of tracking said port request. However Official notice may be taken that the use of such security steps in authorization of port access requests are old and well known in the art. It is common in most personal computer firewalls to implement such steps in authorization of applications to access the Internet for example. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to implement these steps in the system of Saito and Saunders. It would have been desirable to do so as this would increase the security of data processing and data

exchange via a network.

As for claims 58-62, the combination of Saito and Saunders fails to teach a method according to claim 5, wherein the step of providing internal security further comprises: a port request detection step of detecting a port request for use of a port sent by a process; an open port process identification step of, if said port request is an open port request, determining the identity of said requesting process; an open port process check step of, if said port request is an open port request, determining if said process should be permitted to open said port; an open port permit/deny step of, if said port request is an open port request, allowing said open port request to be fulfilled and tracking said open port request if said process should be permitted to open said port and denying said port request if said process should not be permitted to open said port; a close port process completion step of, if said port request is a close port request, completing said port request; and a close port logging step of logging the closing of said port, or where said open port process check step comprises: a secure process list check step of determining whether said process appears on a list of secure processes, or where said tracking of said open port request comprises keeping a log of process ID and returned port handle for said open port request, and said close port logging step of tracking the closing of said port comprises removing from said log said record of process ID and returned port handle for that port close request, or a security check step comprising the steps of checking whether a process has open ports, and denying security clearance for a process with open ports, and allowing security clearance for a

process with no open ports, or wherein said open port process check step of comprises determining if said process identity appears on a secured process list, and where said step of allowing security clearance for a process with no open ports comprises the step of placing said process on said secured process list. However, Official Notice may be taken that the use of such security steps in authorization of port access requests are old and well known in the art. It is common in most personal computer firewalls to implement such steps in authorization of applications to access the Internet for example. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to implement these steps in the system of Saito and Saunders. It would have been desirable to do so as this would increase the security of data processing and data exchange via a network.

As for claims 63-65, the combination of Saito and Saunders fails to teach a method according to claim 5, wherein the step of providing internal security further comprises: a network request detection step of detecting a network request for use of a network sent by a process; a process identification step of determining the identity of said requesting process; a process check step of determining if said process should be permitted to access said network; and a permit/deny step of allowing said network request to be fulfilled if said process should be permitted to access said network and denying said network request: if said process should not be permitted to access said network, or wherein said process check step comprises: a secure process list check step of determining whether said process appears on a list of secure processes, or

wherein said network requests interface is the D Transport Data Interface. However, Official Notice may be taken that the use of such security steps in authorization of port access requests are old and well known in the art. It is common in most personal computer firewalls to implement such steps in authorization of applications to access the Internet for example. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to implement these steps in the system of Saito and Saunders. It would have been desirable to do so as this would increase the security of data processing and data exchange via a network.

11. Claims 66–68 are rejected under 35 U.S.C. 103(a) as being unpatentable over Saito and Schneck US 5,933,498.

As for claim 66, Saito teaches all of the limitations of claim 1 upon which claim 66 depends, but does not teach: receiving a file of data for packaging; receiving a permissions database having one or more permissions associated with the file of data, the one or more permissions governing a client's use of the file; generating a package global unique identifier; generating a package of data comprising the file, the one or more permissions and the global unique identifier; encrypting the package; and generating a computer executable file comprising the encrypted package. However Schneck does teach these features (fig.s 1-3, col. 13 lines 17-27, col. 29 lines 27-57). Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate the features of Schneck into the system of Saito. Motive to

make this combination is found for example, at col. 2 lines 18-27 where the desirability of copyright control systems allowing distributors control of end user use of copyrighted materials is discussed.

As for claim 67, Saito does not teach the method of claim 66 wherein the one or more permissions are selected from the group consisting of: an access count permission, an access time permission, an expiration date permission, an authorization date permission, a clipboard permission, a print permission, an unlimited access permission, an application permission, and a system-events permission. Schneck does teach this feature however, in fig. 3. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate the features of Schneck into the system of Saito. Motive to make this combination is found for example, at col. 2 lines 18-27 where the desirability of copyright control systems allowing distributors control of end user use of copyrighted materials is discussed.

As for claim 68, the combination of Saito and Schneck does not teach the method of claim 67 further comprising the step of setting a password for access to the computer executable file. However Official Notice may be taken that the use of such an access password for encrypted files is a step that is old and well known in the art of digital data distribution. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate these features into the system of Saito and Schneck. It would have been desirable to do so as this would allow for greater

control of end user access to the encrypted content.

Allowable Subject Matter

12. Claims 7, 9-39, 48-54, 69-94, 98-128, and 149 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

13. Claims 131-147 would be allowable if rewritten to overcome the rejection(s) under 35 U.S.C. 112, 2nd paragraph, set forth in this Office action and to include all of the limitations of the base claim and any intervening claims.

Conclusion

14. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paul E. Callahan whose telephone number is (571) 272-3869. The examiner can normally be reached on M-F from 9 to 5.

If attempts to reach the examiner by telephone are unsuccessful, the Examiner's supervisor, Emmanuel Moise, can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is: (571) 273-8300.

Paul Callahan
3-30-06

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER